CLAIMS

1. A method for generating a user attestation-signature value (DAA') for use with a verification computer (40), the user attestation-signature value (DAA') corresponding to at least one attribute (A, B, C, D), each with an attribute value (w, x, y, z), none, one, or more of the attribute values (w, y) remaining anonymous for transactions performable by a user device (20) having a security module (22) with the verification computer (40), the method comprising the steps of:

- providing a user public key (PK_{UC}) and a proof value that demonstrates that the user public key (PK_{UC}) was validly derived from a module public key (PK_{TPM}) of the security module (22);

- receiving from an attester computer (30)

(I) an attestation value (*cert*) having the at least one attribute (A, B, C, D) with its attribute value (w, x, y, z), none, one or more of the attribute values (x, y) remaining unknown to the attester computer (30),

the attestation value (*cert*) being derived from an attester secret key (SK_{AC}), a user public key (PK_{UC}), and none, one, or more attester determined attribute values (w, z),

the user public key (PK_{UC}) inherently comprising none, one, or more user determined attribute values (x, y), and

(II) at least one of the attester determined attribute values (w, z); and

- deriving the user attestation-signature value (DAA') from the attestation value (*cert*) and a security module attestation value (DAA) provided by the security module (22),

wherein it is verifiable whether or not (i) the user attestation-signature value (DAA') was validly derived from the security module attestation value (DAA) and the attestation value (*cert*), and that (ii) the attestation value (*cert*) is associated with a subset (B, D) of at least one attribute, each attribute in the subset (B, D) having a revealed attribute value (x, z).

2. The method according to claim 1, wherein the step of deriving the user attestation-signature value (DAA') further comprises the steps of:

receiving from the security module (22) a first security module attestation value (*T'*$_1$);

deriving an intermediate user attestation-signature value (*C'*) from the first security module attestation value (*T'*$_1$) under use of an attester public key (PK$_{AC}$) and a hash function;

providing the intermediate user attestation-signature value (*C'*) to the security module (22);

receiving from the security module (22) a part of the user attestation-signature value (DAA); and

calculating by the user device (20) further parts of the user attestation-signature value (DAA') using none, one, or more of the attribute values (w, y), the received part of the user attestation-signature value (DAA), the user public key (PK$_{UC}$), and the attester public key (PK$_{AC}$).

3. The method according to claims 1 and 2, wherein the user public key (PK$_{UC}$) is derived from the module public key (PK$_{TPM}$) by using the attester public key (PK$_{AC}$) and the one or more of the attribute values (x, y).

4. The method according to any of the claims 1 to 3, wherein the user device (20) provides encryptions under a trusted third party's public key of one or more of the attribute values (w, y) that remain unknown to the verification computer (40).

5. A method for issuing an attestation value (*cert*) for the generation of a user attestation-signature value (DAA') corresponding to at least one attribute (A, B, C, D), each with an attribute value (w, x, y, z), none, one, or more of the attribute values (w, y) remaining anonymous for transactions performable by a user device (20) having a security module (22) with an attester computer (30), the method comprising the steps of:

- receiving from the user device (20) a user public key (PK$_{UC}$) that inherently comprises none, one, or more user determined attribute values (x, y) invisible to the attester computer (30) and a proof value demonstrating that the user public key (PK$_{UC}$) was validly derived from a module public key (PK$_{TPM}$) of the security module (22);

- issuing the attestation value (*cert*) based on an attester secret key (SK_{AC}), the received user public key (PK_{UC}), and none, one, or more attester determined attribute values (w, z); and

- providing the attestation value (*cert*) to the user device (20),

wherein the user attestation-signature value (DAA') is derivable by the user device (20) from the attestation value (*cert*) and a security module attestation value (DAA) provided by the security module (22), and it is verifiable whether or not (i) the user attestation-signature value (DAA') was validly derived from the security module attestation value (DAA) and the attestation value (*cert*), and that (ii) the attestation value (*cert*) is associated with a subset (B, D) of at least one attribute, each attribute in the subset (B, D) having a revealed attribute value (x, z).

6. A method for verifying a user attestation-signature value (DAA') generated from an attestation value (*cert*), the user attestation-signature value (DAA') corresponding to at least one attribute (A, B, C, D), each with an attribute value (w, x, y, z), none, one or more of the attribute values (w, y) remaining anonymous for transactions performable with a user device (20) having a security module (22), the method comprising the steps of:

- receiving from the user device (20) the user attestation-signature value (DAA'); and

- verifying whether or not (i) the user attestation-signature value (DAA') was validly derived from a security module attestation value (DAA) provided by the security module (22) and an attestation value (*cert*), and (ii) the attestation value (*cert*) is associated with a subset (B, D) of at least one attribute, each attribute in the subset (B, D) having a revealed attribute value (x, z),

the attestation value (*cert*) being derived from an attester secret key (SK_{AC}), a user public key (PK_{UC}), and at least one attribute value (w, z) that remains anonymous,

the user public key (PK_{UC}) inherently comprising a user determined attribute value (x, y).

7. Method according to claim 6, wherein the step of verifying further comprises

computing a first user attestation-signature verification value (*G'*) by using the user attestation-signature value (DAA'), the attester public key (PK_{AC}), and the revealed attribute values (x, z); and

checking whether or not the first user attestation-signature verification value (*G'*) is comprised in the user attestation-signature value (DAA').

8. A computer program element comprising program code means for performing the method of any one of the claims 1 to 7 when said program is run on a computer.

9. A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform the method according to any one of the claims 1 to 7.

10. A system for using a user attestation-signature value (DAA') that corresponds to at least one attribute (A, B, C, D), each with an attribute value (w, x, y, z), none, one, or more of the attribute values (x, y) remaining anonymous for transactions, the system comprising:

a user device (20) having a security module (22) that provides a module public key (PK_{TPM}) and a security module attestation value (DAA), the user device (20) providing a user public key (PK_{UC}) that inherently comprises none, one, or more user determined attribute values (x, y) and a proof value demonstrating that the user public key (PK_{UC}) is validly derived from the module public key (PK_{TPM}) of the security module (22);

an attester computer (30) that provides none, one, or more attester determined attribute values (w, z) and an attestation value (*cert*) that bases on an attester secret key (SK_{AC}), the user public key (PK_{UC}), and the none, one, or more attester determined attribute values (w, z); and

a verification computer (40) for verifying whether or not (i) the user attestation-signature value (DAA') was validly derived from the security module attestation value (DAA) provided by the security module (22) and the attestation value (*cert*), and (ii) the attestation value (*cert*) is associated with a subset (B, D) of at least one attribute, each attribute in the subset (B, D) having a revealed attribute value (x, z).

* * *